REMARKS/ARGUMENTS

Favorable reconsideration of this application in light of the following discussion is respectfully requested.

Claims 1-12 are pending in the application. Claims 1, 7, 9 and 11 are amended by the present amendment. Claims 7 and 11 are amended to correct minor informalities, and support for amended independent Claims 1 and 9 can be found in the original specification, claims and drawings.[1] No new matter is presented.

In the Final Official Action of August 23, 2005, Claims 1-6 and 9-10 were rejected under 35 U.S.C. § 103 as unpatentable over Levergood et al. (U.S. Patent No. 5,708,780, hereinafter "Levergood") in view of "Ericsson Helps Speed Up Mobile Browsing" (InfoWorld article published May 31, 1999, hereinafter "Ericsson"); and Claims 7, 8, 11 and 12 were rejected under 35 U.S.C. § 103 as unpatentable over Levergood and Ericsson and in further view of Wan (U.S. Patent No. 6,044,069).

The Final Action rejected Claims 1-6 and 9-10 under 35 U.S.C. § 103 as unpatentable over Levergood in view of Ericsson. Applicant respectfully submits that amended independent Claims 1 and 9 recite novel features neither taught, nor rendered obvious by the applied references.

Amended independent Claim 1 relates to an authentication server which executes user authentication between a mobile information terminal and a content providing server connected by a data network. In advance of authentication, unique identification information stored in the mobile information terminal is registered with a customer database of an authentication server. This unique identification information, which is stored in the mobile information terminal, corresponds to the hardware of the terminal and identifies a manufacturer of the mobile terminal. In an exemplary non-limiting embodiment, as

[1] e.g., specification, p. 11.

described at p. 11 of the specification, the identification information corresponds to a "flash ID" that is stored in the flash memory of the mobile device and is unique to each mobile information terminal of each manufacturer. Thus, the "flash ID" is unique to each mobile terminal and essentially permanently associated with each terminal.

This unique identification information is encrypted by a predetermined encryption algorithm and supplied from the mobile information terminal, via the network, and decoded by the authentication server. The server determines whether the unique identification information decoded in the decoding step is registered with the customer database, and notifies the content providing server to facilitate the start of services for the mobile information terminal.

This method allows a user of a mobile information terminal, or mobile phone, to be authenticated by without having to transmit additional information, such as a password and user name to be authenticated at a server. The flash ID is simply retrieved from the device and authentication is performed based on this unique identifier stored in, and associated with, the hardware of the device.

Turning to the applied primary reference, Levergood describes a process for controlling and monitoring access to network servers via client-server sessions over a network. Specifically, Levergood describes that a client request, without a session identification (SID), is sent from a web browser and directed to an access controlled file, and a content server subjects the client to an authorization routine prior to issuing the SID.[2] In order to obtain a valid SID, the user must first be authenticated by an account database (216) using various non-encrypted parameters. If the user is authorized, a SID is generated allowing the user to gain access to the content. [3]

[2] Levergood, col. 3, lines 21-27.
[3] Id, col. 6, line 58-col. 9, line 6.

However, Levergood fails to teach or suggest registering unique hardware specific identification information identifying a manufacturer of the terminal at a customer database and transmitting this customer identification information to the customer database to gain access to content.

Specifically, Claim 1 recites, *inter alia*, user authentication method, comprising:

> ...registering unique identification information ***corresponding to the hardware*** of said mobile information terminal with a customer database of said authentication server in advance, ***wherein said unique identification information is stored in said mobile information terminal and comprises information identifying a manufacturer of the mobile information terminal;***
>
> decoding the unique identification information encrypted by a predetermined encryption algorithm and supplied from said mobile information terminal via said open network;
>
> ***determining whether the unique identification information decoded in the decoding step is registered with said customer database...***

In contrast, Levergood describes that information such as client IP address and password, as well as user demographic information, such as user age, home address, hobby or occupation may be stored in the content server and associated with a user.[4] This information is registered in the authentication server, thus allowing the user of Levergood's system to be issued a SID to receive requested content. However, the device of Levergood requires that user-specific information be sent over the network each time the user requests content, and also requires that a different SID is issued and stored in the terminal device to receive specific content. The transmission of personal information poses an inconvenience (typing a username and password; forgetting a username and password) and a security risk (repeatedly transmitting personal information over the open network) for the user.

The system of amended Claim 1 allows a user to register user information, including the unique identification information at a customer database, and use only the unique hardware identification information for authentication. Then when the user wishes to access

[4] Levergood at col. 6, lines 60-65.

a network location requiring authentication with the customer database, the unique identification information is retrieved from memory, encrypted, and sent to the customer database for user authentication. Thus, the user is not required to enter personal information, or manually type in a username and password in order to easily gain access to premium content for which they are registered. The hardware unique information is anonymous to a user, does not change and allows the user to seamlessly and transparently authenticate with an customer database, as described, for example, at p. 19-21 of the specification. Levergood fails to teach or suggest registering such hardware unique information, or exchanging such information for registration and authentication. Thus, using unique identification information ***corresponding to the hardware*** of said mobile information terminal which ***is stored in said mobile information terminal and comprises information identifying a manufacturer of the mobile information terminal***, and exchanging such information for registration and authentication provides a distinct advantage over Levergood, as Levergood fails to teach or suggest these claimed features.

Further, as Ericsson is relied upon only to describe the ability of a mobile phone to connect over the internet to a server device, Applicant respectfully submits that Ericsson fails to teach or suggest any of the above-noted features recited in amended Claim 1.

Accordingly, Applicant respectfully requests the rejection of Claim 1 under 35 U.S.C. § 103 be withdrawn. For substantially the same reasons as given with respect to Claim 1, it is also submitted that Claim 9 patentably defines over Levergood and/or Ericsson.

Claims 7, 8, 11 and 12 were rejected under 35 U.S.C. § 103 as unpatentable over Levergood, Ericsson and in further view of Wan. Applicant respectfully traverses this rejection.

As discussed above, Levergood, neither alone nor in combination with Ericsson, teach or suggest the above distinguished features recited in amended independent Claims 1 and 9.

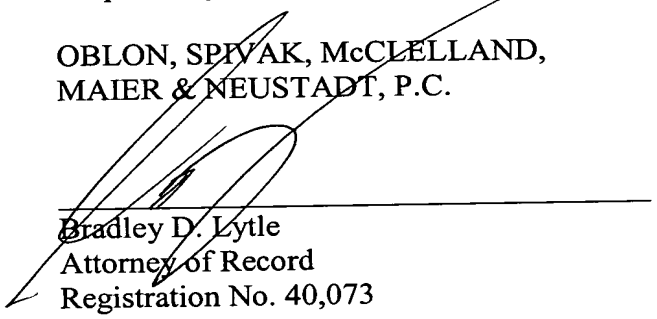
Likewise, Wan fails to remedy this deficiency, and therefore, none of the cited references either alone or in combination, teach or suggest Applicant's Claims 7, 8, 11 and 12 which include the above distinguished features by virtue of dependency. Therefore, the applied references fail to provide a *prima facie* case of obviousness with regard to any of these claims.

Accordingly, Applicant respectfully requests the rejection of Claims 7, 8, 11 and 12 under 35 U.S.C. § 103 be withdrawn.

Consequently, in light of the foregoing comments, it is respectfully submitted that the invention defined by Claims 1-12 is patentably distinguishing over the applied references. The present application is therefore believed to be in condition for formal allowance and an early and favorable reconsideration of the application is therefore requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Andrew T. Harry
Registration No. 56,959

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)
ATH:smi

I:\ATTY\ATH\PROSECUTION\21'S\212668-US\212668US-AM 12-23-05.DOC